

INTERNET PROTOCOL FILTER

Patent number: JP11508753T

Publication date: 1999-07-27

Inventor:

Applicant:

Classification:

- international: H04L12/56; G06F13/00; H04L12/28; H04L12/46;
H04L12/66; H04L29/06

- european: H04L12/46B; H04L29/06; H04L29/06C6A; H04L29/12A

Application number: JP19970537534T 19970423

Priority number(s): WO1997CA00269 19970423; US19960015945P
19960424

Also published as:

WO9740610 (A3)
WO9740610 (A2)
EP0895684 (A3)
EP0895684 (A2)
EP0895684 (B1)

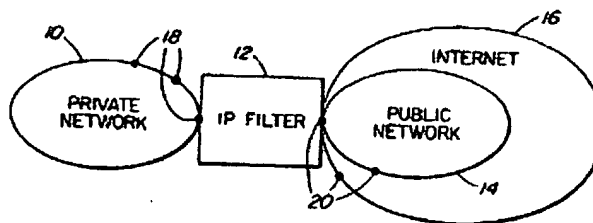
more >>

Report a data error here

Abstract not available for JP11508753T

Abstract of corresponding document: **WO9740610**

The IP filter (12), embodying the present invention, is a communications device designed to provide public network (14) or Internet (16) access to nodes (18) of private networks (10), advantageously without requiring the private nodes on such networks to register public Internet addresses. The IP filter presents a single IP address to the Internet and uses a plurality of IP ports to solve the problem of IP address conservation. It initiates sessions by assigning private side IP sessions to a unique port of the IP filter's public address. The IP filter effects a translation between a source port number for the private network and a destination port number for the public network for communication therebetween. Benefits of the IP filter include private node security and conservation of Internet-registered addresses.



Data supplied from the **esp@cenet** database - Worldwide

(19)日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11)特許出願公表番号

特表平11-508753

(43)公表日 平成11年(1999) 7月27日

(51)Int.Cl. ⁶	識別記号	F I	
H 0 4 L 12/56		H 0 4 L 11/20	1 0 2 A
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 Z
H 0 4 L 12/28		H 0 4 L 11/20	B
12/46		13/00	3 0 5 Z
12/66		11/00	3 1 0 C
		審査請求 有	予備審査請求 有 (全 41 頁) 最終頁に続く

(21)出願番号 特願平9-537534
 (86) (22)出願日 平成9年(1997) 4月23日
 (85)翻訳文提出日 平成10年(1998)10月22日
 (86)国際出願番号 PCT/CA97/00269
 (87)国際公開番号 WO97/40610
 (87)国際公開日 平成9年(1997)10月30日
 (31)優先権主張番号 60/015, 945
 (32)優先日 1996年4月24日
 (33)優先権主張国 米国 (US)
 (81)指定国 EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, L U, MC, NL, PT, SE), AU, CA, CN, J P, KR

(71)出願人 ノーザン・テレコム・リミテッド
 カナダ国, エイチ2ワイ 3ワイ4, ケベック, モントリオール, エステイ. アントイン ストリート ウェスト 380 ワールドトレード センタ オブ モントリオール 8フロア
 (72)発明者 ウットン・ブルース・アンソニー
 アメリカ合衆国, 27613, ノースカロライナ州, ラレイ, ベントツイグドライブ 10601
 (74)代理人 弁理士 泉 和人

最終頁に続く

(54)【発明の名称】 インターネット・プロトコル・フィルタ

(57)【要約】

本発明のIPフィルタ(12)は、公衆ネットワーク(14)またはインターネット(16)アクセスをプライベート・ネットワーク(10)のノードに提供するために設計された通信デバイスである。ネットワーク上のプライベート・ノードを公衆インターネット・アドレスに登録する必要性がない利点がある。IPフィルタはインターネットに単一のIPアドレスを与え、複数のIPポートを使ってIPアドレス管理の問題を解決している。これはプライベート側のIPセッションをIPフィルタの公衆アドレスの単一ポートに割り当てることによってセッションを始める。IPフィルタはプライベート・ネットワーク向けのソース・ポート番号と、公衆ネットワーク向けの宛先ポート番号間の翻訳を行う。IPフィルタの利点はプライベート・ノード・セキュリティ、インターネットに登録されたアドレス管理にある。

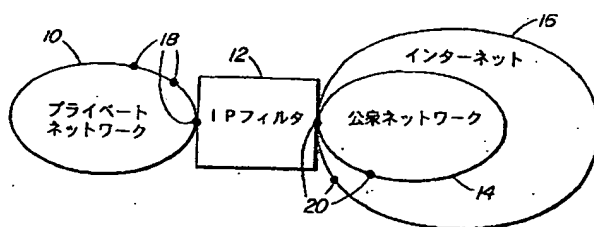


FIG. 1

【特許請求の範囲】

1. 公衆ネットワーク内で知られたアドレスを有するフィルタ・ノードを介してプライベート・データ通信ネットワーク(10)と公衆データ通信ネットワーク(14)をインタフェースする方法において:

プライベート・ネットワーク内のノード(18)からフィルタ・ノードへ宛先情報とソース情報を含んだデータ・パケットをルーティングし、この宛先情報は、公衆ネットワーク内のノード(20)に対応する宛先アドレスと宛先ポートを含み、そのソース情報は、各プライベート・ネットワーク・ノードのソース・アドレスとソース・ポート含み、

フィルタ・ノードでプライベート・ネットワークから受信された各データ・パケットは、フィルタ・ノードのポートを表わす単一の値と相関関係のあるデータ・パケットから抽出されたソース情報を含み、データ・パケット内でソース・アドレスをフィルタ・ノード・アドレスに置き換え、ソース・ポートをフィルタ・ノード・ポート値に置き換え、

公衆ネットワーク内で、各宛先情報に従って、置き換えられたソース情報を含むデータ・パケットをフィルタ・ノードから対応の公衆ネットワーク・ノードにルーティングすることを特徴とする通信ネットワーク・インタフェース方法。

2. 請求項1記載の方法において:

フィルタ・ノードのアドレスを有するデータ・パケット・アドレスを宛先アドレスとして公衆ネットワーク内のノードからフィルタ・ノードにルーティングし、

フィルタ・ノード、公衆ネットワークから受信した各データ・パケットに対して、データ・パケット内の宛先情報の宛先ポートを特定のソース情報に相関させ、データ・パケット内で、宛先情報を特定のソース情報で置き換え、

プライベート・ネットワーク内で、置き換えられた宛先情報を有するデータ・パケットをフィルタ・ノードから対応するプライベート・ネットワーク・ノードにルーティングすることを特徴とする通信ネットワーク・インタフェース方法。

法。

3. 請求項2記載の方法において：

データ・パケット内の宛先情報の宛先ポートが、維持されているソース情報と相関がない場合は、フィルタ・ノードは公衆ネットワークから受信したデータ・パケットを無視することを特徴とする通信ネットワーク・インタフェース方法。

4. 請求項3記載の方法において：

ソース情報を保持するステップは、
各データ・パケットからのソース情報をルックアップ・テーブル中にエントリとしてストアし、ソース情報に相関するフィルタ・ノード・ポート値は、エントリ用のテーブル中にインデックスを構成することを特徴とする通信ネットワーク・インタフェース方法。

5. 請求項4記載の方法において：

データ・パケットはインターネット・プロトコル（IP）上で送信制御プロトコル（TCP）に従ったパケットを含むことを特徴とする通信ネットワーク・インタフェース方法。

6. 請求項5記載の方法において：

フィルタ・ノードで、プライベート・ネットワークからのTCPパケットを受信し、TCPパケットに対応するエントリがルックアップ・テーブルに見つからず、TCPパケットが「これは接続リクエストである」と示した場合、ソース情報とTCPパケットからの宛先情報を新しいエントリとしてルックアップ・テーブルにストアすることを特徴とする通信ネットワーク・インタフェース方法。

7. 請求項6記載の方法において：

フィルタ・ノードで、公衆ネットワークからのTCPパケットを受信し、受信されたTCPパケット内のソース・ポートがTCPパケット内の宛先ポートによってインデックスされたルックアップ・テーブルのソース情報エントリ内の宛先ポートと異なり、TCPパケットが「このパケットは接続リクエストに対する最初の応答である」と示した場合、フィルタ・ノードはテーブル・エントリ内の宛先ポートをTCPパケットから受信されたソース・ポートに更新することを特

徴とする通信ネットワーク・インタフェース方法。

8. 請求項7記載の方法において：

フィルタ・ノードで、パケット内に送信コードの終端を有するTCPパケットを受信し、受信されたTCPパケットに対応するルックアップ・テーブル内のエントリをゼロにすることを特徴とする通信ネットワーク・インタフェース方法。

9. 請求項4記載の方法において：

データ・パケットはインターネット・プロトコル(IP)上でユーザ・データグラム・プロトコル(UDP)に従ったパケットを含むことを特徴とする通信ネットワーク・インタフェース方法。

10. 請求項9記載の方法において：

フィルタ・ノードで、プライベート・ネットワークからのUDPデータ・パケットを受信し、ルックアップ・テーブル内の新しいエントリとして、UDPパケットからのソース情報と宛先情報を経過タイマの期間表示と共に追加すること

11. プライベート・データ通信ネットワーク(10)と公衆データ通信ネットワーク(14)をフィルタ・ノードを介してインタフェースする方法において：

(a) フィルタ・ノードで、公衆ネットワーク内のノード(20)に対応した宛先アドレスと、プライベート・ネットワーク内のノード(18)に対応したソース・アドレスを有するデータ・パケットをプライベート・ネットワークか

ら受信し、

(b) フィルタ・ノードで、データ・パケットから抽出したソース・アドレスを維持し、

(c) データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスと置き換え、

(d) 公衆ネットワーク内で、宛先アドレスに従って、置き換えられたソース・アドレスを有するデータ・パケットをフィルタ・ノードから対応する公衆

ネットワーク・ノードにルーティングし、

(e) 置き換えられたソース情報を有するデータ・パケットに応答して公衆ネットワークからの戻りパケットを待ち、

(f) 戻りパケット内で、宛先アドレスを維持されたソース・アドレスと置き換え、

(g) プライベート・ネットワーク内で、置き換えられた宛先アドレスを有する戻りパケットをフィルタ・ノードから対応するプライベート・ネットワーク・ノードへルーティングすることを特徴とする通信ネットワーク・インタフェース方法。

12. 請求項11記載の方法において：

フィルタ・ノードにおいて、戻りパケットを待っている間に、プライベート・ネットワークから受信されたデータ・パケットをさらにバッファリングし、バッファされたパケットがあればそのパケットに対して、ステップ(b)から(g)を繰り返すことを特徴とする通信ネットワーク・インタフェース方法。

13. 請求項12記載の方法において：

データ・パケットはインターネット制御メッセージ・プロトコル(ICMP)に従ったパケットを含むことを特徴とする通信ネットワーク・インタフェース方法。

14. 第1のデータ通信ネットワーク(10)および第2のデータ通信ネットワーク(14)をインタフェースするフィルタ・ノード(12)を動作させる方法において：

宛先情報とソース情報を有するデータパケットを第1のネットワークから受信し、その宛先情報は、第2のネットワーク内のノード(20)に対応する宛先アドレスと宛先ポートを有し、そのソース情報は、第1のネットワーク内のノード(18)に対応するソース・アドレスとソース・ポートを有し、

フィルタ・ノードのポートを表わす唯一の値と相関関係のあるデータ・パケットから抽出されたソース情報を維持し、

データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスに

置き換え、ソース・ポートをフィルタ・ノード・ポート値と置き換え、

置き換えられたソース情報を有するデータ・パケットを第2のネットワークに送り、それによってそのパケットは宛先情報に従って対応する第2のネットワーク・ノードにルーティングされることを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

15. 請求項14記載の方法において：

フィルタ・ノードのアドレスを有するデータ・パケットを宛先アドレスとして第2のネットワークから受信し、

データ・パケット内の宛先情報の宛先ポートを、保持されている特定のソース情報に相関させ、

データ・パケット内で、宛先情報を特定のソース情報と置き換え、

置き換えられた宛先情報を有するデータ・パケットを第1のネットワークに送り、それによってそのパケットが宛先情報に従って対応の第1のネットワーク・ノードにルーティングされることを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

16. 請求項15記載の方法において：

そのデータ・パケット内の宛先情報の宛先ポートが、維持されたソース情報と相関がなかった場合、第2のネットワークから受信されたデータ・パケットを

無視することを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

17. 請求項16記載の方法において：

ソース情報を維持するステップは、データ・パケットからのソース情報をルックアップ・テーブルにエントリとしてストアし、ソース情報に相関するフィルタ・ノード・ポート値は、エントリ用のテーブルにインデックスを構成すること、を特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

18. 請求項17記載の方法において：

データ・パケットはインターネット・プロトコル(IP)上で送信制御プロ

トコル (T C P) に従ったパケットを含むことを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

19. 請求項18記載の方法において：

第1のネットワークからT C Pパケットを受信し、そのT C Pパケットに対応するエントリがルックアップ・テーブルに見つからず、そのT C Pパケットが「これは接続リクエストである」と示した場合、ソース情報をT C Pパケットからの宛先情報と共に、ルックアップ・テーブル内の新しいエントリとしてストアすることを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

20. 請求項19記載の方法において：

第2のネットワークからT C Pパケットを受信し、受信されたT C Pパケット内のソース・ポートが、T C Pパケット内の宛先ポートによってインデックスされたルックアップ・テーブルのソース情報エントリ内の宛先ポートと異なり、またT C Pパケットが「このパケットが接続リクエストに対する最初の応答である」ことを示した場合には、テーブル・エントリ内の宛先ポートを受信したT C

Pパケットからのソース・ポートで更新することを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

21. 請求項20記載の方法において：

パケット内の送信コードの終端を有するT C Pパケットを受信し、受信されたT C Pパケットに対応するルックアップ・テーブル内のエントリをゼロにすることことを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

22. 請求項17記載の方法において：

データ・パケットはインターネット・プロトコル (I P) 上でデータグラム・プロトコル (U D P) に従ったパケットを含むことを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

23. 請求項22記載の方法において：

第1のネットワークからのU D Pデータ・パケットを受信し、ルックアップ

・テーブル内の新しいエントリとして、UDP パケットからのソース情報と宛先情報を経過タイマの期間表示と共に追加することを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

24. 第1のデータ通信ネットワーク(10)と第2のデータ通信ネットワーク(14)をインタフェースするフィルタ・ノード(14)を動作させる方法において:

(a) 第2のネットワーク内のノード(20)に対応する宛先アドレスと第1のネットワーク中のノード(18)に対応するソース・アドレスとを有するデータ・パケットを第1のネットワークから受信し、

(b) データ・パケットから抽出されたソース・アドレスを維持し、

(c) データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスと置き換え、

(d) 置き換えられたソース・アドレスを有するデータ・パケットを第2のネットワークに送り、それによってそのパケットは対応の第2のネットワーク・ノードにルーティングされ、

(e) 置き換えられたソース情報を有するデータ・パケットに応じて、第2のネットワークからの戻りパケットを受信し、

(f) 戻りパケット内で、宛先アドレスと維持されたソース・アドレスとを置き換え、

(g) 置き換えられた宛先アドレスを有する戻りパケットを第1のネットワークに送り、それによってそのパケットは対応の第1のネットワーク・ノードにルーティングされることを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

25. 請求項24記載の方法において:

戻りパケットを待つ間に第1のネットワークから受信されたデータ・パケットをバッファリングし、バッファされたパケットがあった場合には、それぞれに対しステップ(b)から(g)を繰り返すことを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

26. 請求項 25 記載の方法において：

データ・パケットはインターネット制御メッセージ・プロトコル (I C M P) に従ったパケットを含むことを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

27. 第 1 のデータ通信ネットワーク (1 0) と第 2 のデータ通信ネットワーク (1 4) をインタフェースするフィルタ・ノード (1 2) において：

第 2 のネットワーク内のノード (2 0) に対応する宛先アドレスと宛先ポートを有する宛先情報と、第 1 のネットワーク内のノード (1 8) に対応するソース・アドレスとソース・ポートを有するソース情報とを有するデータパケットを第 1 のネットワークから受信する手段と、

フィルタ・ノードのポートを表わす唯一の値と相関関係のあるデータ・パケットから抽出されたソース情報を維持する手段と、

データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスに置き換え、ソース・ポートをフィルタ・ノード・ポート値と置き換える手段と、

置き換えられたソース情報を有するデータ・パケットを第 2 のネットワークに送り、それによってそのパケットを宛先情報に従って対応の第 2 のネットワーク・ノードにルーティングする手段とを備えたことを特徴とするフィルタ・ノード。

28. 請求項 27 記載のフィルタ・ノードにおいて：

フィルタ・ノードのアドレスを有するデータ・パケットを宛先アドレスとして第 2 のネットワークから受信する手段と、

データ・パケット内の宛先情報の宛先ポートを、保持されている特定のソース情報に相関させる手段と、

データ・パケット内で、宛先情報を特定のソース情報と置き換える手段と、

置き換えられた宛先情報を有するデータ・パケットを第 1 のネットワークに送り、それによってそのパケットを宛先情報に従って対応の第 1 のネットワーク・ノードにルーティングする手段とを備えたことを特徴とするフィルタ・ノード。

29. 請求項28記載のフィルタ・ノードにおいて：

そのデータ・パケット内の宛先情報の宛先ポートが、維持されたソース情報と相関がなかった場合、第2のネットワークから受信されたデータ・パケットを無視する手段を備えたことを特徴とするフィルタ・ノード。

30. 請求項29記載のフィルタ・ノードにおいて：

ソース情報を維持するステップは、データ・パケットからのソース情報をルックアップ・テーブルにエントリとしてストアする手段を備え、そのソース情報に相関するフィルタ・ノード・ポート値は、エントリ用のテーブルにインデックスを構成することを特徴とするフィルタ・ノード。

31. 第1のデータ通信ネットワーク(10)と第2のデータ通信ネットワーク(14)をインタフェースするフィルタ・ノード(12)において：

(a) 第2のネットワーク内のノード(20)に対応する宛先アドレスと第1のネットワーク中のノード(18)に対応するソース・アドレスとを有するデータ・パケットを第1のネットワークから受信する手段と、

(b) データ・パケットから抽出されたソース・アドレスを維持する手段と、

(c) データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスと置き換える手段と、

(d) 置き換えられたソース・アドレスを有するデータ・パケットを第2のネットワークに送り、それによってそのパケットを対応の第2のネットワーク・ノードにルーティングする手段と、

(e) 置き換えられたソース情報を有するデータ・パケットに応じて、第2のネットワークからの戻りパケットを受信する手段と、

(f) 戻りパケット内で、宛先アドレスと維持されたソース・アドレスとを置き換える手段と、

(g) 置き換えられた宛先アドレスを有する戻りパケットを第1のネットワークに送り、それによってそのパケットを対応の第1のネットワーク・ノードにルーティングする手段とを備えたことを特徴とするフィルタ・ノード。

32. 請求項 31 記載のフィルタ・ノードにおいて：

戻りパケットを待つ間に第 1 のネットワークから受信されたデータ・パケットをバッファリングし、バッファされたパケットがあった場合には、それぞれに対しステップ (b) から (g) を繰り返す手段を備えたことを特徴とするフィルタ・ノード。

【 発 明 の 詳 細 な 説 明 】

発 明 の 名 称

インターネット・プロトコル・フィルタ

発 明 の 分 野

本発明は一般的に、インターネット・ファイアウォールに関する。特に、プライベート・インターネット・プロトコル (IP) ネットワーク・ドメインを公衆インターネット上の単一 IP アドレスにマッピングするインターネット・プロトコル・フィルタに関する。

背 景 技 術

ファイアウォールは、一般的に、プライベート・ネットワークのドメイン内のノードをインターネットのような公衆ネットワーク内のノードに結びつける機能を有するコンピュータサーバとして知られ、特徴づけられる。公知のファイアウォール製品の欠点として、セッションの同時発生または公衆ノードとプライベート・ノード間の相互作用に対して、独自の公衆 IP アドレスが必要になることが知られている。このため、公衆 IP アドレスを管理するファイアウォールが望まれていた。

発 明 の 概 要

本発明の目的は、2つのネットワーク間の通信を結合する新しい改良された装置を提供することにある。

本発明の第1の側面によると、本発明は、公衆ネットワーク内で知られたアドレスを有するフィルタ・ノードを介してプライベート・データ通信ネットワークと公衆データ通信ネットワークをインタフェースする方法において：プライベート・ネットワーク内のノードからフィルタ・ノードへ宛先情報とソース情報を含んだデータ・パケットをルーティングし、この宛先情報は、公衆ネットワーク内のノードに対応する宛先アドレスと宛先ポートを含み、そのソース情報は、各プライベート・ネットワーク・ノードのソース・アドレスとソース・ポート含み、フィルタ・ノードでプライベート・ネットワークから受信された各データ・パケットは、フィルタ・ノードのポートを表わす単一の値と相関関係のあるデータ・

パケットから抽出されたソース情報を含み、データ・パケット内でソース・アドレスをフィルタ・ノード・アドレスに置き換え、ソース・ポートをフィルタ・ノード・ポート値に置き換え、公衆ネットワーク内で、各宛先情報に従って、置き換えられたソース情報を含むデータ・パケットをフィルタ・ノードから対応の公衆ネットワーク・ノードにルーティングするように構成される。

本発明の第2の側面によれば、本発明は、プライベート・データ通信ネットワークと公衆データ通信ネットワークをフィルタ・ノードを介してインタフェースする方法において：(a) フィルタ・ノードで、公衆ネットワーク内のノードに対応した宛先アドレスと、プライベート・ネットワーク内のノードに対応したソース・アドレスを有するデータ・パケットをプライベート・ネットワークから受信し、(b) フィルタ・ノードで、データ・パケットから抽出したソース・アドレスを維持し、(c) データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスと置き換え、(d) 公衆ネットワーク内で、宛先アドレスに従って、置き換えられたソース・アドレスを有するデータ・パケットをフィルタ・ノードから対応する公衆ネットワーク・ノードにルーティングし、(e) 置き換えられたソース情報を有するデータ・パケットに応答して公衆ネットワークからの戻りパケットを待ち、(f) 戻りパケット内で、宛先アドレスを維持されたソース・アドレスと置き換え、(g) プライベート・ネットワーク内で、置き換えられた宛先アドレスを有する戻りパケットをフィルタ・ノードから対応するプライベート・ネットワーク・ノードへルーティングするように構成される。

本発明の第3の側面によれば、本発明は、第1のデータ通信ネットワークおよび第2のデータ通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法において：宛先情報とソース情報を有するデータパケットを第1のネットワークから受信し、その宛先情報は、第2のネットワーク内のノードに対応

する宛先アドレスと宛先ポートを有し、そのソース情報は、第1のネットワーク内のノードに対応するソース・アドレスとソース・ポートを有し、フィルタ・ノードのポートを表わす唯一の値と相関関係のあるデータ・パケットから抽出されたソース情報を維持し、データ・パケット内で、ソース・アドレスをフィルタ・

ノードのアドレスに置き換え、ソース・ポートをフィルタ・ノード・ポート値と置き換え、置き換えられたソース情報を有するデータ・パケットを第 2 のネットワークに送り、それによってそのパケットは宛先情報に従って対応する第 2 のネットワーク・ノードにルーティングされるように構成される。

本発明の第 4 の側面によれば、本発明は、第 1 と第 2 のデータ通信をインタフェースするフィルタ・ノードを提供する。このフィルタ・ノードは、フィルタ・ノードのアドレスを有するデータ・パケットを宛先アドレスとして第 2 のネットワークから受信する手段と、データ・パケット内の宛先情報の宛先ポートを、保持されている特定のソース情報に相関させる手段と、データ・パケット内で、宛先情報を特定のソース情報と置き換える手段と、置き換えられた宛先情報を有するデータ・パケットを第 1 のネットワークに送り、それによってそのパケットを宛先情報に従って対応の第 1 のネットワーク・ノードにルーティングする手段とを備えるように構成される。

本発明で実現される IP フィルタは、公衆ネットワークやインターネット・アクセスをプライベート・ネットワークのノードに供給するために設計された通信デバイスである。IP フィルタは、ネットワーク上でプライベート・ノードを必要とせず、公衆インターネット・アドレスに登録できることを利点とする。IP フィルタはインターネットに単一 IP アドレスを与え、複数の IP ポートを使って IP アドレス管理の問題を解決する。IP フィルタはプライベート側の IP セッションを IP フィルタの公衆アドレスの単一ポートに割り当てることによってセッションを開始する。これによって最大で 64,512 (65,536-1,024 ポート) の同時セッションが単一 IP アドレスでサポートされる。IP フィルタはプライベート・ネットワーク用のソース・ポート番号と、公衆ネットワーク用の宛先ポ

ート番号間で通信を行うための翻訳を行う。IP フィルタはプライベート・ノードのセキュリティ、インターネットに登録されたアドレス管理などに利点がある。

特定の実施の形態として、IP フィルタはインターネット・プロトコル上で 3 つのデータ伝送プロトコルをサポートできる。送信コントロールプロトコル (TCP)、ユーザ・データグラム・プロトコル (UDP)、およびインターネット

制御メッセージ・プロトコル (I C M P) の 3 つである。他のプロトコルのパケットは無視される。

T C P プロトコルは T C P ヘッダをデータ・パケットに付加する。ソース・ポートと宛先ポートの番号はこのヘッダ内に含まれる。ソース・ノードと宛先ノードのインターネット・アドレスは I P ヘッダ内に含まれる。各パケットから抽出された I P アドレスとポート情報を使って、I P フィルタはこのパケットをどこにルーティングするかを決定する。

I P フィルタは各 T C P 接続上で情報のルックアップ・テーブルを保持する。この情報にはプライベート・ノードからのポート、プライベート I P アドレス、宛先ノードの割り当てポート番号、I P フィルタのポート番号をインデックスの形で含んでいる。パケットをプライベート・ネットワークから受け取ると、このパケットに対応するエントリがテーブル中に見つからず、T C P ヘッダが「これは新しい接続リクエストである」ことを示した場合、プライベート・アドレスとポート番号は新しいエントリとしてテーブルに追加される。その後、パケット・ヘッダ内のソース・アドレスとポート番号は I P フィルタの I P アドレスとポート番号に置き換えられ、パケットはインターネットに送信される。

I P フィルタは、インターネットからパケットを受け取ると、宛先ポート番号を使ってルックアップ・テーブルにインデックスを付ける。対応のテーブル・エントリが見つかり、宛先アドレスとポート番号はプライベート・ネットワークの I P アドレスとポート番号に置き換えられ、パケットはプライベート・ネット

ワークに送信される。受け取ったパケットのソース・ポートがテーブルに記録されたポートと異なる場合、またパケット・ヘッダ情報が「このパケットは接続上で最初の応答である」ことを示した場合、ルックアップ・テーブルは必要に応じてインターネット・ノードによって割り当てられたポート番号で更新される。

I P フィルタがパケット内で送信コードの終わりを検出すると、ルックアップ・テーブル・エントリは 0 にリセットされる。I P フィルタが I P フィルタ・ポートに対応するルックアップ・テーブルの中にエントリを持たないインターネットからパケットを受け取ると、I P フィルタはそのパケットを無視する。

UDP プロトコルは TCP とは逆に、接続レス、または接続指向プロトコルである。UDP ヘッダは初期接続または送信終了を制御するコードを含まない。UDP ヘッダ内で関係のあるデータはソース・ポートと宛先ポートである。この情報は IP ヘッダに含まれたインターネット情報を共に使用され、IP フィルタがどこにパケットをルーティングするかを決める。

IP フィルタは各 UDP セッション上で情報のルックアップ・テーブルを保持する。IP フィルタがプライベート・ネットワークから UDP パケットを受け取ると、IP フィルタはソース・アドレス、ソース・ポート番号、宛先ポート番号、および割り当てられた IP フィルタ・ポート番号をテーブルのインデックスとして記録する。次にパケット・ヘッダ内のプライベート・ノード・アドレスとポート番号は、IP フィルタのアドレスと割り当てポート番号に置き換えられる。その後、パケットはインターネットに送信される。

IP フィルタがインターネットから UDP パケットを受け取ると、IP フィルタは UDP ルックアップ・テーブルにインデックスをつけ、パケットの宛先情報つまり IP フィルタ・アドレスと割り当てポート番号を、ルックアップ・テーブルからのプライベート・アドレスとポート番号に置き換える。ルックアップ・テーブルは、また、標準 UDP の実行によって受け取ったデータグラム・パケット

上の経過タイマの期間表示を保持する。IP フィルタが IP フィルタ・ポートに対応するルックアップ・テーブルの中でエントリを持たないインターネットからのパケットを受け取ると、フィルタはそのパケットを無視する。

ICMP パケットはソース・ポート番号も宛先ポート番号も持っていないので、プライベート・ネットワークから受け取った ICMP パケットは 1 度に 1 つだけ、追加 ICMP パケットのバッファリングで処理される。IP フィルタはパケット・ヘッダからプライベート・アドレスを読み、それを IP フィルタのアドレスと置き換える。パケットはインターネットに送信され、IP フィルタは応答を待つ。IP フィルタが応答パケットを受け取ると、パケット・ヘッダ内の宛先アドレスは IP フィルタの宛先アドレスからプライベート・ネットワーク上のノードの宛先アドレスに変わる。次に IP フィルタはこのパケットをプライベート・

ネットワークに送信する。

I P プロトコル上でパケットを問題なく送信するためには、各ノードは他のホストの I P アドレスとイーサネットベースのデータ通信ネットワーク内のそれに対応するイーサネット・アドレスのテーブルを保持していなければならない。ノードは実際には I P アドレスとイーサネット・アドレスを使ってパケットをアドレスする。この2つのアドレスの関係はダイナミックであり、すなわち、I P アドレスを有するノードはイーサネット・アドレスを変えることができる。アドレス・テーブル内の情報は、A R P パケットのノードの放送に対する応答から得られる。ソース・ノードは A R P パケットを放送し、宛先ノードの I P が与えられ、宛先ノードのイーサネット・アドレスをリクエストする。宛先ノードがパケットを受け取ると、その宛先ノードはリクエストされた情報を有する応答パケットを送る。

I P フィルタは、真の A R P テーブルを保持していないが、T C P と U D P のパケット通過と同じ方法で、A R P パケットを送る。I P フィルタが公衆ネットワークの宛先を有するプライベート・ネットワーク上のノードから A R P パケッ

トを受け取ると、ソース・アドレス情報をフィルタのアドレス情報に置き換える。プライベート・ノードの I P アドレスとターゲット I P アドレスはルックアップ・テーブルの中に入れられる。ターゲット・ノードがそれ自身のイーサネット・アドレスで応答すると、宛先アドレス情報は I P フィルタの情報からプライベート・ノードの情報に変わり、その後パケットがプライベート・ノードに送信される。プライベート・ノード・アドレス情報はテーブルから得られる。A R P パケットがファイアウォールに向けられていると、A R P パケットは I P フィルタを通らず、フィルタと相手のネットワークの間で通信が遮断される。

I P フィルタによって生じるイベントやエラーはログとして登録され、たとえば、テキスト・ファイルの中に記録される。

理想的には、I P フィルタはネットワークからパケットを受け取ってすぐに処理するのが望ましいが、ネットワーク通信が過負荷の場合、I P フィルタはパケットをプライベート・ネットワーク用とインターネット用の2つの待ち行列の中

にバッファリングする。

2つのソース・ルックアップ・テーブルと宛先ルックアップ・テーブルを、前者はTCPパケット用、後者はUDPパケット用に使用してもよい。各テーブルは、通信セッションに割り当てられたIPフィルタ・ポート番号によって直接インデックスされる。テーブルのエントリはプライベート・ノードのIPアドレス、プライベート・ノードのソース・ポート、およびインターネット・ノードの宛先ポートを含む。特定のIPフィルタ・ポートに接続がない場合、テーブル中の対応のエントリは0にリセットされる。プライベート・ネットワークとインターネットの両方から到着したパケットは同じルックアップ・テーブルを使って処理される。この構成では、使用可能なIPフィルタ通信ポートの中でパケットのいくつかの宛先がUDPに、いくつかの宛先がTCPに指定されていると仮定している。

図面の簡単な説明

本発明は、添付の図面および次の説明から理解される。

図1はプライベート・ネットワークと公衆ネットワークを結合する1つのインターネット・プロトコルフィルタを表す概略図である。

図2はフィルタ内部のコンポーネントを表わすブロック図である。

発明の実施の形態

図1は、インターネット・プロトコル(IP)フィルタ12を通じて公衆ネットワーク14に接続されるプライベート・ネットワーク10を示す図である。この公衆ネットワーク14はインターネット16とも呼ばれるグローバル・データ・ネットワークの一部を形成する。プライベート・ネットワーク10は、ローカルエリア・ネットワーク(LAN)のような既存のデータ通信ネットワークを表し、プライベート・ネットワークのドメイン内で単一のIPアドレスによって識別される複数のノード18を有する。公衆ネットワーク14とインターネット16は公衆ドメインデータ通信ネットワークを表し、それぞれ対応するIPアドレスを有する複数のノード20を有する。

IPフィルタ12はゲートウェイとして機能し、そこを通してデータ・パケッ

トがプライベート・ネットワーク 10 と公衆ネットワーク 14 間で交換され、それによってプライベート・ネットワーク 10 のノード 18 にインターネット・アクセスを行う。IP フィルタ 12 はプライベート・ネットワーク・ノード 18 の 1 つを構成し、インターネットに登録された公衆 IP アドレスを有する唯一のノードである。これによって IP フィルタ 12 は本質的に公衆ノード 20 の 1 つをも構成し、その IP アドレスは公衆ドメイン内で知られる。他のプライベート・ネットワーク・ノード 18 の IP アドレスはプライベート・ネットワーク 10 に対して保存され、公衆インターネット・アドレス・ドメイン内では知られず、登録もされない。従来と同様、IP フィルタ 12 の関連 IP アドレスは複数の IP ポートであり、全部で 65,536 あり、そのうち特に 64,512 は既定のプロトコル用に保存されず、アドレスの翻訳のために使うことができる。

プライベート・ネットワーク 10 上のノード 18 間の通信は、IP フィルタ 12 の存在によって影響を受けることはないが、公衆ネットワーク 14、特にその中のノード 20 にアクセスするために、プライベート・ノード 18 はすべての通信リクエストを、IP フィルタ 12 を通してルーティングする。IP フィルタ 12 は、プライベート・ノード 18 とインターネット・ノード 20 間の通信を、プライベート・ネットワーク 10 から受け取ったデータ・パケットのヘッダ情報を修正することによって管理し、その後各通信を公衆ネットワーク 14 に送信する。この修正によりプライベート・ノード 18 と公衆インターネット・ノード 20 間の通信は、実際には IP フィルタ 12 とインターネット・ノード 20 間の通信になり、すべての戻り通信を IP フィルタ 12 にルーティングし、次に、戻りデータ・パケットをプライベート・ノード 18 にルーティングする。

IP フィルタ 12 は、公衆ネットワーク 14 からは接続リクエストを受け取らない。プライベート・ノード 18 と公衆ノード 20 間の通信はすべて、プライベート・ノード 18 によって始められる。IP フィルタ 12 はインターネット・プロトコル上で TCP、UDP および ICMP メッセージの 3 つのデータ伝送プロトコルをサポートするように設計されており、他のプロトコルのパケットは拒否されるか無視される。

翻訳テーブルはIPフィルタ12によって保持され、プライベート・ネットワーク10から受信した公衆ネットワーク14向けの packets に対するアドレスとポートをマッピングする。翻訳テーブルは各エントリに対して以下の項目を含む。

プライベートIPアドレス	(p I P)
プライベートポート	(p P o r t)
インターネット (公衆) IPアドレス	(i I P)
インターネット (公衆) ポート	(i P o r t)
タイマ	
セッションのタイプ/状態	

イーサネット・アドレス

基本的な翻訳は、プライベート・ネットワーク側からのIPアドレスとポートをIPフィルタのIPアドレスとポートに置き換え、これによってプライベート・ネットワーク10上のすべてのノードを公衆ネットワーク14から隠す。

プライベート・ネットワーク側からの packets は、ソースと宛先 (p I P 、 p P o r t → i I P 、 i P o r t) を指定する。

これは「ソケット」を定義し、その中で接続の両端 (ソースと宛先) はIPヘッダ内のIPアドレスとTCPまたはUDPヘッダ内のポートによって定義される。

IPフィルタ12は上記を (f r I P 、 f r P o r t → i I P 、 i P o r t) のように翻訳する。

ここで f r I P は公衆ネットワーク14上のIPフィルタ12のIPアドレスであり、 f r P o r t は翻訳テーブル+オフセット値へのインデックスである。このオフセット値は、たとえば、1024であり、よく知られたポートを使ってスキップする。 f r P o r t は任意のポートを表わす。

インターネット・ノード20は次の packets で返答する。

(i I P 、 i P o r t → f r I P 、 f r P o r t)

これをIPフィルタ12が受け取り、次のように翻訳する。

(i I P 、 i P o r t - p I P 、 p P o r t)

一般的にプライベート側から翻訳するには、(プロトコルタイプ、p I P 、 p P o r t 、 i I P 、 i P o r t) の値は翻訳テーブルの中になければならない。これはハッシュ・テーブルを参照して行う必要がある。

公衆側からの翻訳は、直接テーブルを表をして行うことができる。f r P o r t - 1 0 2 4 はテーブルへのインデックスであるからである。パケット内の (i

I P 、 i P o r t) がテーブル中の対応するエントリにマッチしていない場合、承認されていないアクセスは登録され、パケットは捨てられる。

翻訳パケット内でポートがT C PまたはU D Pヘッダ内で置き換えられると、T C P / U C P と I P ヘッダ内のチェックサムを再計算しなければならない。I P アドレスが I P ヘッダの中で置き換えられると、I P ヘッダチェックサムを再計算しなければならない。

以下は I P フィルタ 1 2 がサポートする異なるプロトコルについて、特に注意すべき点である。

T C P の場合、S Y N パケットをプライベート・ネットワーク 1 0 から受け取ると、I P フィルタ 1 2 は使われていないエントリをテーブル中に入れ、その中を埋め、タイプをT C P に、状態をS Y N に設定する。その後パケットは上記の一般的な構成によって送られる。テーブル中に空のエントリがないとパケットは捨てられ、イベントが登録される。

S Y N パケットを公衆ネットワーク 1 4 インタフェースから受け取ると、それは、認可されないものとして扱われ、登録される (但し、以下のようなF T P の特別のケースは除く)。しかし、翻訳テーブル・エントリの状態がS Y N の場合にはS Y N + A C K パケットが送られる。このようなパケットを送った後、状態はO P E N に設定される。

I P フィルタがF I N パケットを受け取り、翻訳テーブル内の状態がF I N でなかった場合、その状態はF I N に設定され、そのパケットは送られる。状態がF I N の場合、パケットは送られ翻訳テーブル・エントリは 0 に設定することによって削除される。F I N はそれぞれの側に送られ、T C P 接続は終了する。R

S T パケットを受け取ると、翻訳テーブル・エントリは削除される。

U D P プロトコルに関し、いずれかの U D P パケットをプライベート・ネットワーク 1 0 側から受け取ると、I P フィルタ 1 2 は、まず標準的な参照を試みる。翻訳テーブル・エントリが見つからない場合には、使われないエントリが設定され、状態は O P E N に設定される。空のエントリがブランク中に見つからない場合には、パケットを捨てる代わりにテーブル中のランダム U D P が上書きされる。U D P は非接続で信頼できない送信であるので、エントリの上書きが必要であったパケットを公衆ネットワーク 1 4 から受け取ると、そのパケットは捨てられ、プライベート側上のノード 1 8 は再度試みを行う。

F T P に関し、F T P クライアントは、ポート 2 1 などの特定のポート上の F T P サーバと T C P 「制御」接続を確立する。しかしながら、データを送信する必要がある場合、F T P サーバは、たとえば、デフォルトでは 2 0 になっている「データ」ポートからの T C P 接続を、クライアントが指定した宛先ポートにオープンにする。

これをサポートするために、プライベート・ネットワーク 1 0 からポート 2 0 に送られたパケットは、I P フィルタ 1 2 で F T P 「ポート」コマンドに対して分析される必要がある。検出された場合、テーブル中の新しいエントリを、p P o r t を用いて、F T P ポート・コマンド内の値に設定しなければならない。F T P コマンド内の I P アドレスとポート番号は、パケットを送る前に、I P フィルタのアドレスとポートに変換しなければならない。状態は F T P D A T A に設定される。

S Y N パケットを公衆ネットワーク 1 4 から受け取り、テーブル・エントリが存在して F T P D A T A 状態にある場合、パケットは送られ、状態は O P E N に設定される。

I C M P プロトコルに関し、I C M P パケットをプライベート・ネットワーク 1 0 から受け取ると、そのパケットがエコー・リクエスト（ピング）の場合、I

P フィルタ 1 2 は、新しいエントリを翻訳テーブルの中に置く。パケットのシー

ケンス・フィールドはテーブル中の `p P o r t` に保存され、テーブル・インデックスはパケットのシーケンス・フィールド内に置かれる。ICMP チェックサムは再計算され、標準 IP ヘッダの置換が行われる。このタイプは ICMP、状態は P I N G に設定され、タイマは 1 分に設定される。

エコー応答（ピング）を公衆ネットワーク 14 のインタフェースから受け取ると、シーケンス・フィールドはテーブルへのインデックスとして使われる。状態が P I N G の場合、テーブル中の `p P o r t` はパケットのシーケンス・フィールドに置き換えられ、ICMP チェックサムが再計算され、標準 IP ヘッダの置き換えが行われる。その後、テーブル・エントリは削除される。

エコー・リクエスト（ピング）を公衆ネットワーク 14 から受信すると、IP フィルタ 12 が応答する。これによってインターネット・アクセスが可能になり IP フィルタ 12 に到達し、IP フィルタ 12 が実行されていることが確認できる。

宛先に到達できなかったパケットを公衆ネットワーク 14 から受け取ると、含まれているヘッダ情報が抽出される。プロトコルが TCP または UDP であった場合、送信側のパケットの (`f r I P`、`f r P o r t` - `i I P`、`i P o r t`) が決定され翻訳テーブル・エントリの位置が決められる。ICMP から抽出された IP アドレスが、テーブル中のアドレスにマッチしていた場合、IP フィルタ 12 は、標準の構成を使ってパケットをプライベート・ネットワーク 10 に送る。その他の ICMP パケットは、どちらの側から送られたものでも捨てられ、登録される。

ほとんどのデータ通信プロトコルは UDP プロトコルまたは TCP プロトコルに基づいているので、クライアントへの戻り接続をサーバにオープンさせる FTP のように交渉を始めない限り、これらの他のプロトコルは IP フィルタ 12 と

互換性がある。他に互換性のあるプロトコルは、T e l n e t、T F T P（小さなファイル送信プロトコル）、D N S（ドメイン名サービス）、およびウェブブラウザなどである。

パケットはどちらの方向に送られても、翻訳テーブル・エントリ内のタイマ・

フィールドは計算タイムアウト値（ピングを除く）に設定される。テーブル中にあるすべてのアクティブ・エントリのタイマ・フィールドは1分きざみで減少し、0になると、翻訳テーブル・エントリは削除される。これによって、もはや使われていないUDPエントリとPINGエントリ、また、不正に終了してFINをどちらの側にも送っていないTCPエントリが消去される。使われていないエントリをテーブル中に長く置いておくと安全上問題になる可能性がある。適切な計算タイムアウト値は、典型的なTCPの時間より少しだけ長いものである。

特定の実施の形態では、プライベート・ネットワーク10と公衆ネットワーク14はイーサネットベースのLANである。IPフィルタ12は、データ処理プラットフォームによって実行され、このプラットフォームはそれぞれネットワーク10と14に接続された2つの既存のイーサネット・ハードウェア・インタフェースを備えており、適当なソフトウェアを備え、IPフィルタ12の機能を実行する。

図2は、データ処理プラットフォームによって実行できるソフトウェアという点から見たIPフィルタ12の内部コンポーネントを示す図である。内部コンポーネントは2つのパケットドライバ30と32、アドレス解像プロトコル（ARP）テーブル34、イーサネット・アドレス・テーブル36、IPハンドラ38、アドレス翻訳器40およびユーザ・インタフェース42を含む。パケットドライバ30と32はイーサネット・ハードウェア・インタフェースを制御し、それぞれプライベート・ネットワーク10と公衆ネットワーク14と通信する。IPハンドラ38はメッセージを送受信するためのルータ機能を提供し、ARPテーブル34とイーサネット・テーブル36を保持する。アドレス翻訳器40は、プ

ラ
イベート・ネットワーク10からのソース・ポート番号と、公衆ネットワーク側14上の宛先ポート番号間の翻訳を行う。

ユーザ・インタフェース42は、処理プラットフォームに付属したキーボードとディスプレイ端末を用いてオペレータがIPフィルタ12にインタフェースすることを可能にする。ファンクションキーは、IPフィルタを計算したり、ログ

ファイルを見たり、コピーしたり、状態を表示したりする。ログファイルはTCPまたはUDPセッションの接続時間、入出力トラフィックの統計、IPフィルタ12への無効アクセスを含む。ログファイルが大きくなりすぎるのを防ぐために、情報は日付が変わると新しいファイルに登録される。

パケットとIPフィルタ12間のルーティングについては、公衆ネットワーク14の観点からは公衆インタフェースについて、プライベート・ネットワーク10の観点からはプライベート・インタフェースについて、以下に記述する。

公衆インタフェースは、LANセグメント上でホストとして機能する。公衆インタフェースはパケットを送るために、宛先IPがローカルLANセグメント上にあるかどうかを確認する。ローカルLANセグメント上にあった場合、公衆インタフェースはその中のARPテーブル中でイーサネット・アドレスを探す。ARPテーブル中にエントリがない場合、公衆インタフェースはパケットを待ち行列に置き、ARPリクエストを送ってイーサネット・アドレスを取得しなければならない。ARPテーブル・エントリの標準エージングアウトを実行する必要がある。IP宛先がLANセグメント上にない場合、公衆インタフェースはパケットを計算されたデフォルトのルータに送る。デフォルトルータから送られたICMPリダイレクトメッセージは無視される。

プライベート・インタフェースは、パケットを1つまたは複数のルータに送り遠隔クライアントのステーションと通信する必要があるため、ルータの機能に影響を与える。大きな遠隔クライアント・ネットワークは、複数のルータマシンに

アクセスする場合がある。以前のルート割り当てではルート割り当てエントリがサブネット・アドレスではなくホスト・アドレスになっていたため、ルート割り当てテーブルも大きくなる可能性があった。すなわち、クライアントがルータ1またはルータ2からアクセスできるように設定されているネットワークでは、どのルータもクライアント・ステーションがあるサブネットのルータにはなれないということである。ルート・テーブルをプライベート・ネットワーク上のすべてのルータからRIPを通じて取得するこれまでのルータでは、接続された各遠隔クライアントは大きなホスト・アドレス・テーブルを必要とした。これはルート

を探すために必要な検索時間、巨大なテーブルに必要なメモリ、すべてのルータ間のLANセグメント上のRIPトラフィックの性能に影響を与える可能性もある。

この環境の中でルーティングを行うために、IPフィルタはイーサネット・テーブルを保持する。プライベート側から公衆側に送られるすべてのパケットに対して翻訳エントリが存在している場合は、イーサネット・インデックスを使って入ってきたパケットのイーサネット・ソース・アドレスと比較する。2つが一致すれば、他の作業は必要ない。一致しなければ、イーサネット・テーブルを検索してソース・イーサネット・アドレスを探し、見つからない場合には新しいイーサネット・テーブル・エントリを追加する。その後、イーサネット・テーブルへのインデックスは、翻訳テーブル・エントリの中に保存される。その後、パケットが公衆側からプライベート側へ翻訳されると、イーサネット・アドレスは翻訳テーブルのインデックスから直接検索することができる。このようにしてパケットはルータへルーティングされ、このルータはパケットをIPフィルタに送る。

当業者であれば、本発明の特許請求の範囲から逸れることなく、本発明の実施の形態に対して、さまざまな修正、変更、応用が可能である。したがって、各実施の形態に関し特定の制限がない場合、請求項は上記の実施の形態に制限されることはない。

【 図 1 】

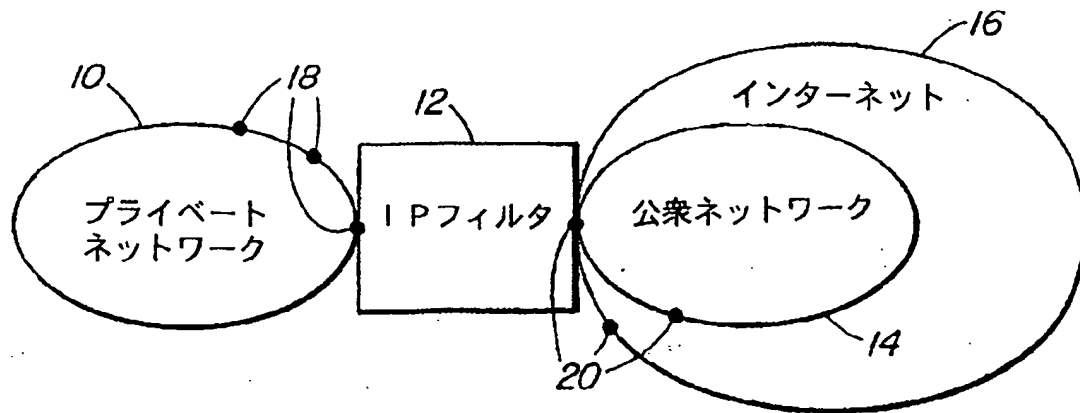


FIG. 1

【 図 2 】

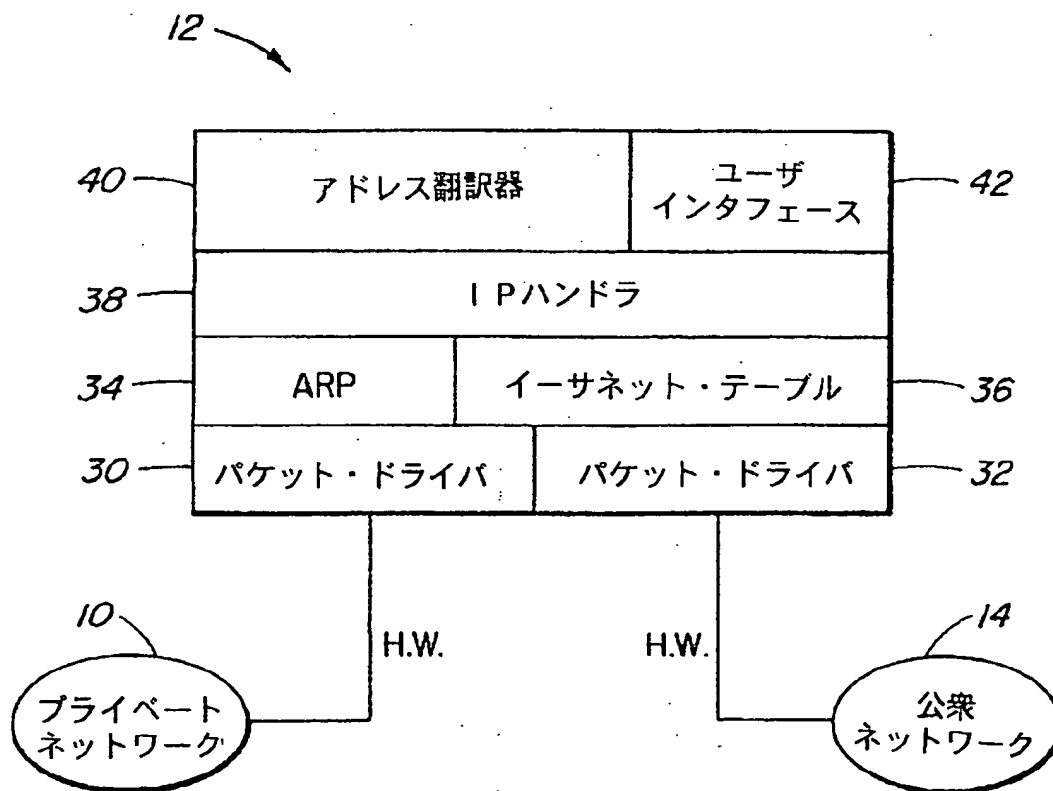


FIG. 2

【手続補正書】特許法第184条の8第1項

【提出日】1998年4月20日

【補正内容】

明細書

発明の名称

インターネット・プロトコル・フィルタ

発明の分野

本発明は一般的に、インターネット・ファイアウォールに関する。特に、プライベート・インターネット・プロトコル（IP）ネットワーク・ドメインを公衆インターネット上の単一IPアドレスにマッピングするインターネット・プロトコル・フィルタに関する。

背景技術

ファイアウォールは、一般的に、プライベート・ネットワークのドメイン内のノードをインターネットのような公衆ネットワーク内のノードに結びつける機能を有するコンピュータサーバとして知られ、特徴づけられる。

エゲバング等は、1994年5月、アメリカのインターネットエンジニアリング・タスクフォースの、論文「IPネットワーク・アドレス・トランスレータ（NAT）」中で、ファイアウォールとして機能するネットワークアドレストランスレータ（NAT）を発表した。このNATは、たとえば、プライベートネットワークのようなIPスタブ・ドメイン、およびインターネットのような公衆ネットワークドメインの端に置かれる。NAT内のテーブルは一对のローカルIPアドレス、すなわち、スタブ・ドメインに対してはローカルで、グローバルには唯一のアドレスであるホストのアドレスから成り立っている。スタブドメイン内のローカルIPアドレスはグローバルには唯一ではない。スタブドメイン内のホストが公衆ネットワークドメインを介した通信を必要とする場合、そのローカルIPアドレスは、テーブルからグローバルに唯一なIPアドレスの1つとペアになっている。ペアになっているグローバルに唯一なIPアドレスは、ホストのローカルIPアドレスの代わりに公衆ネットワークドメイン内の通信に使われ、これによ

って、一定レベルのセキュリティをホストに提供する。

公知のファイアウォール製品の欠点として、セッションの同時発生または公衆ノードとプライベート・ノード間の相互作用に対して、独自の公衆IPアドレスが必要になることが知られている。このため、公衆IPアドレスを管理するファイアウォールが望まれていた。

発明の概要

本発明の目的は、2つのネットワーク間の通信を結合する新しい改良された装置を提供することにある。

本発明の第1の側面によると、本発明は、第1のデータ通信ネットワークおよび第2のデータ通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法において：宛先情報とソース情報を有するデータパケットを第1のネットワークから受信し、その宛先情報は、第2のネットワーク内のノードに対応する宛先アドレスと宛先ポートを有し、そのソース情報は、第1のネットワーク内のノードに対応するソース・アドレスとソース・ポートを有し、フィルタ・ノードのポートを表わす唯一の値と相関関係のあるデータ・パケットから抽出されたソース情報を維持し、データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスに置き換え、ソース・ポートをフィルタ・ノード・ポート値と置き換え、置き換えられたソース情報を有するデータ・パケットを第2のネットワークに送り、それによってそのパケットは宛先情報に従って対応する第2のネットワーク・ノードにルーティングされるように構成される。

本発明の第2の側面によれば、本発明は、第1のデータ通信ネットワークと第2のデータ通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法において：(a)第2のネットワーク内のノードに対応する宛先アドレスと第1のネットワーク中のノードに対応するソース・アドレスとを有するデータ・パケットを第1のネットワークから受信し、(b)データ・パケットから抽出されたソース・アドレスを維持し、(c)データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスと置き換え、(d)置き換えられたソース・アドレスを有するデータ・パケットを第2のネットワークに送り、それによってそのパケ

ットは対応の第2のネットワーク・ノードにルーティングされ、(e)置き換えられたソース情報を有するデータ・パケットに応じて、第2のネットワークからの戻りパケットを受信し、(f)戻りパケット内で、宛先アドレスと維持されたソース・アドレスとを置き換え、(g)置き換えられた宛先アドレスを有する戻りパケットを第1のネットワークに送り、それによってそのパケットは対応の第1のネットワーク・ノードにルーティングされるように構成される。

本発明の第3の側面によれば、本発明は、第1のデータ通信ネットワークと第2のデータ通信ネットワークをインタフェースするフィルタ・ノードにおいて：第2のネットワーク内のノードに対応する宛先アドレスと宛先ポートを有する宛先情報と、第1のネットワーク内のノードに対応するソース・アドレスとソース・ポートを有するソース情報とを有するデータパケットを第1のネットワークから受信する手段と、フィルタ・ノードのポートを表わす唯一の値と相関関係のあるデータ・パケットから抽出されたソース情報を維持する手段と、データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスに置き換え、ソース・ポートをフィルタ・ノード・ポート値と置き換える手段と、置き換えられたソース情報を有するデータ・パケットを第2のネットワークに送り、それによってそのパケットを宛先情報に従って対応の第2のネットワーク・ノードにルーティングする手段とを備えるように構成される。

本発明の第4の側面によると、本発明は、第1のデータ通信ネットワークと第2のデータ通信ネットワークをインタフェースするフィルタ・ノードにおいて：
(a) 第2のネットワーク内のノードに対応する宛先アドレスと第1のネットワーク中のノードに対応するソース・アドレスとを有するデータ・パケットを第1のネットワークから受信する手段と、(b)データ・パケットから抽出されたソース・アドレスを維持する手段と、(c)データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスと置き換える手段と、(d)置き換えられたソース・アドレスを有するデータ・パケットを第2のネットワークに送り、それによってそのパケットを対応の第2のネットワーク・ノードにルーティングする手段と、(e)置き換えられたソース情報を有するデータ・パケットに応じて、第2のネ

ネットワークからの戻りパケットを受信する手段と、(f)戻りパケット内で、宛先アドレスと維持されたソース・アドレスとを置き換える手段と、(g)置き換えられた宛先アドレスを有する戻りパケットを第1のネットワークに送り、それによってそのパケットを対応の第1のネットワーク・ノードにルーティングする手段とを備えるように構成される。

本発明で実現されるIPフィルタは、公衆ネットワークやインターネット・アクセスをプライベート・ネットワークのノードに供給するために設計された通信デバイスである。IPフィルタは、ネットワーク上でプライベート・ノードを必要とせず、公衆インターネット・アドレスに登録できることを利点とする。IPフィルタはインターネットに単一IPアドレスを与え、複数のIPポートを使ってIPアドレス管理の問題を解決する。IPフィルタはプライベート側のIPセッションをIPフィルタの公衆アドレスの単一ポートに割り当てることによってセッションを開始する。これによって最大で64,512(65,536-1,024ポート)の同時セッションが単一IPアドレスでサポートされる。IPフィルタはプライベート・ネットワーク用のソース・ポート番号と、公衆ネットワーク用の宛先ポート番号間で通信を行うための翻訳を行う。

請求の範囲

1. 第1のデータ通信ネットワークおよび第2のデータ通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法において：

宛先情報とソース情報を有するデータパケットを第1のネットワークから受信し、その宛先情報は、第2のネットワーク内のノードに対応する宛先アドレスと宛先ポートを有し、そのソース情報は、第1のネットワーク内のノードに対応するソース・アドレスとソース・ポートを有し、

フィルタ・ノードのポートを表わす唯一の値と相関関係のあるデータ・パケットから抽出されたソース情報を維持し、

データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスに置き換え、ソース・ポートをフィルタ・ノード・ポート値と置き換え、

置き換えられたソース情報を有するデータ・パケットを第2のネットワーク

に送り、それによってそのパケットは宛先情報に従って対応する第2のネットワーク・ノードにルーティングされることを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

2. 請求項1記載の方法において：

フィルタ・ノードのアドレスを有するデータ・パケットを宛先アドレスとして第2のネットワークから受信し、

データ・パケット内の宛先情報の宛先ポートを、保持されている特定のソース情報に相関させ、

データ・パケット内で、宛先情報を特定のソース情報と置き換え、

置き換えられた宛先情報を有するデータ・パケットを第1のネットワークに送り、それによってそのパケットが宛先情報に従って対応の第1のネットワー

ク・ノードにルーティングされることを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

3. 請求項2記載の方法において：

そのデータ・パケット内の宛先情報の宛先ポートが、維持されたソース情報と相関がなかった場合、第2のネットワークから受信されたデータ・パケットを無視することを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

4. 請求項3記載の方法において：

ソース情報を維持するステップは、データ・パケットからのソース情報をルックアップ・テーブルにエントリとしてストアし、ソース情報に相関するフィルタ・ノード・ポート値は、エントリ用のテーブルにインデックスを構成すること
を特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

5. 請求項4記載の方法において：

データ・パケットはインターネット・プロトコル (IP) 上で送信制御プロトコル (TCP) に従ったパケットを含むことを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

6. 請求項 5 記載の方法において：

第1のネットワークからTCPパケットを受信し、そのTCPパケットに対応するエントリがルックアップ・テーブルに見つからず、そのTCPパケットが「これは接続リクエストである」と示した場合、ソース情報をTCPパケットからの宛先情報と共に、ルックアップ・テーブル内の新しいエントリとしてストアすることを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

7. 請求項 6 記載の方法において：

第2のネットワークからTCPパケットを受信し、受信されたTCPパケット内のソース・ポートが、TCPパケット内の宛先ポートによってインデックスされたルックアップ・テーブルのソース情報エントリ内の宛先ポートと異なり、またTCPパケットが「このパケットが接続リクエストに対する最初の応答である」ことを示した場合には、テーブル・エントリ内の宛先ポートを受信したTCPパケットからのソース・ポートで更新することを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

8. 請求項 7 記載の方法において：

パケット内の送信コードの終端を有するTCPパケットを受信し、受信されたTCPパケットに対応するルックアップ・テーブル内のエントリをゼロにすることことを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

9. 請求項 4 記載の方法において：

データ・パケットはインターネット・プロトコル(IP)上でデータグラム・プロトコル(UDP)に従ったパケットを含むことを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

10. 請求項 9 記載の方法において：

第1のネットワークからのUDPデータ・パケットを受信し、ルックアップ・テーブル内の新しいエントリとして、UDPパケットからのソース情報と宛先情報を経過タイマの期間表示と共に追加することを特徴とする通信ネットワークを

インタフェースするフィルタ・ノードを動作させる方法。

1.1. 第1のデータ通信ネットワークと第2のデータ通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法において：

- (a) 第2のネットワーク内のノードに対応する宛先アドレスと第1のネットワーク中のノードに対応するソース・アドレスとを有するデータ・パケットを第1のネットワークから受信し、
- (b) データ・パケットから抽出されたソース・アドレスを維持し、
- (c) データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスと置き換え、
- (d) 置き換えられたソース・アドレスを有するデータ・パケットを第2のネットワークに送り、それによってそのパケットは対応の第2のネットワーク・ノードにルーティングされ、
- (e) 置き換えられたソース情報を有するデータ・パケットに応じて、第2のネットワークからの戻りパケットを受信し、
- (f) 戻りパケット内で、宛先アドレスと維持されたソース・アドレスとを置き換え、
- (g) 置き換えられた宛先アドレスを有する戻りパケットを第1のネットワークに送り、それによってそのパケットは対応の第1のネットワーク・ノードにルーティングされることを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

1.2. 請求項1.1記載の方法において：

戻りパケットを待つ間に第1のネットワークから受信されたデータ・パケットをバッファリングし、バッファされたパケットがあった場合には、それぞれに対しステップ(b)から(g)を繰り返すことを特徴とする通信ネットワークをインタフェースするフィルタ・ノードを動作させる方法。

1.3. 請求項1.2記載の方法において：

データ・パケットはインターネット制御メッセージ・プロトコル(ICMP)に従ったパケットを含むことを特徴とする通信ネットワークをインタフェースす

るフィルタ・ノードを動作させる方法。

14. 第1のデータ通信ネットワークと第2のデータ通信ネットワークをイン

タフェースするフィルタ・ノードにおいて：

第2のネットワーク内のノードに対応する宛先アドレスと宛先ポートを有する宛先情報と、第1のネットワーク内のノードに対応するソース・アドレスとソース・ポートを有するソース情報とを有するデータパケットを第1のネットワークから受信する手段と、

フィルタ・ノードのポートを表わす唯一の値と相関関係のあるデータ・パケットから抽出されたソース情報を維持する手段と、

データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスに置き換え、ソース・ポートをフィルタ・ノード・ポート値と置き換える手段と、

置き換えられたソース情報を有するデータ・パケットを第2のネットワークに送り、それによってそのパケットを宛先情報に従って対応の第2のネットワーク・ノードにルーティングする手段とを備えたことを特徴とするフィルタ・ノード。

15. 請求項14記載のフィルタ・ノードにおいて：

フィルタ・ノードのアドレスを有するデータ・パケットを宛先アドレスとして第2のネットワークから受信する手段と、

データ・パケット内の宛先情報の宛先ポートを、保持されている特定のソース情報に相関させる手段と、

データ・パケット内で、宛先情報を特定のソース情報と置き換える手段と、

置き換えられた宛先情報を有するデータ・パケットを第1のネットワークに送り、それによってそのパケットを宛先情報に従って対応の第1のネットワーク・ノードにルーティングする手段とを備えたことを特徴とするフィルタ・ノード。

16. 請求項15記載のフィルタ・ノードにおいて：

そのデータ・パケット内の宛先情報の宛先ポートが、維持されたソース情報と相関がなかった場合、第2のネットワークから受信されたデータ・パケットを

無視する手段を備えたことを特徴とするフィルタ・ノード。

17. 請求項 16 記載のフィルタ・ノードにおいて：

ソース情報を維持するステップは、データ・パケットからのソース情報をルックアップ・テーブルにエントリとしてストアする手段を備え、そのソース情報に相関するフィルタ・ノード・ポート値は、エントリ用のテーブルにインデックスを構成することを特徴とするフィルタ・ノード。

18. 第1のデータ通信ネットワークと第2のデータ通信ネットワークをインタフェースするフィルタ・ノードにおいて：

(a) 第2のネットワーク内のノードに対応する宛先アドレスと第1のネットワーク中のノードに対応するソース・アドレスとを有するデータ・パケットを第1のネットワークから受信する手段と、

(b) データ・パケットから抽出されたソース・アドレスを維持する手段と、

(c) データ・パケット内で、ソース・アドレスをフィルタ・ノードのアドレスと置き換える手段と、

(d) 置き換えられたソース・アドレスを有するデータ・パケットを第2のネットワークに送り、それによってそのパケットを対応の第2のネットワーク・ノードにルーティングする手段と、

(e) 置き換えられたソース情報を有するデータ・パケットに応じて、第2のネットワークからの戻りパケットを受信する手段と、

(f) 戻りパケット内で、宛先アドレスと維持されたソース・アドレスとを置き換える手段と、

(g) 置き換えられた宛先アドレスを有する戻りパケットを第1のネットワークに送り、それによってそのパケットを対応の第1のネットワーク・ノードにルーティングする手段とを備えたことを特徴とするフィルタ・ノード。

19. 請求項 18 記載のフィルタ・ノードにおいて：

戻りパケットを待つ間に第1のネットワークから受信されたデータ・パケッ

トをバッファリングし、バッファされたパケットがあった場合には、それぞれに
対しステップ (b) から (g) を繰り返す手段を備えたことを特徴とするフィル
タ・ノード。

【 國際調查報告 】

INTERNATIONAL SEARCH REPORT

Intern. Application No
PCT/CA 97/00269A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L29/06 H04L12/46

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	RFC1631. May 1994. INTERNET ENGINEERING TASK FORCE, USA. pages 1-10, XP002040992 EGEVANG K AND FRANCIS P: "The IP Network Address Translator (NAT)" see paragraph 2; figures 1,2 see paragraph 3.3	1.11.14. 24.27.31
A	EP 0 465 201 A (DIGITAL EQUIPMENT CORP) 8 January 1992 see column 7, line 30 - column 8, line 27 see column 10, line 45 - column 12, line 22; figure 2 --- -/--	1.11.14, 24.27.31

☒ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

Z document member of the same patent family

Date of the actual completion of the international search

19 September 1997

Date of mailing of the international search report

14.10.97

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Authorized officer

Dupuis, H

INTERNATIONAL SEARCH REPORT

Inter. Application No.
PCT/CA 97/00269

C. (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	INTERNET SECURITY HANDBOOK, 1995, MAIDENHEAD, ENGLAND, pages 27-37, XP002040993 STALLINGS W: see page 31; figure 3.2 -----	11,24,31

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No.

PCT/CA 97/00269

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0465201 A	08-01-92	US 5309437 A	03-05-94
		CA 2044363 A	30-12-91
		DE 69122439 D	07-11-96
		DE 69122439 T	15-05-97

フロントページの続き

(51) Int. Cl.⁶

識別記号

F I

H 0 4 L 29/06

(72) 発明者 コルビン・ウィリアム・ジー
カナダ国, エル9ティー 4 ジェイ 6, オ
ンタリオ, ミルトン, チャイルズドライブ
874